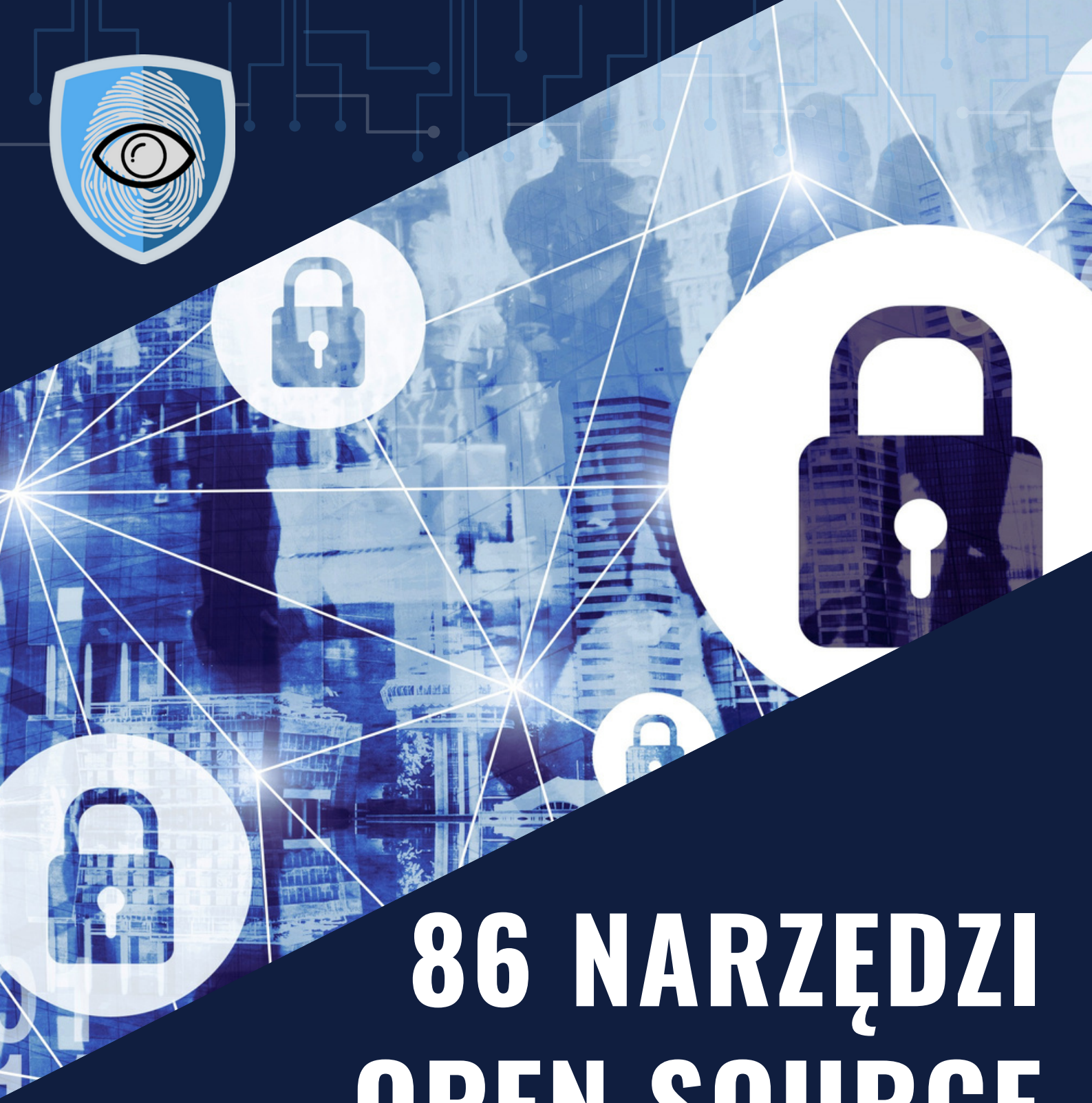

86 NARZĘDZI OPEN SOURCE

KTÓRE UŁATWIĄ CI UTRZYMANIE BEZPIECZEŃSTWA W SYSTEMACH I SIECIACH

Wydawca:
SecurityBezTabu.pl
E-mail: wojtek@securitybeztabu.pl
Kontakt: https://securitybeztabu.pl/kontakt/
Telefon: +48 695 801 020

Miejsce i data wydania: Warszawa, Listopad 2022

Opracowanie graficzne: Wojciech Ciemski
Pomoc organizacyjna: Oskar Klimczuk
Korekta tekstu: Dorota Księżopolska

Patronat:

Resilia
architekci odporności biznesu

Drogi Czytelniku!
Jeżeli chcesz się ze mna podzielić opinią o tej publikacji, napisz do mnie:
wojtek@securitybeztabu.pl

Podziel się swoimi uwagami, spostrzeżeniami lub recenzją.

Resilia
architekci odporności biznesu

SECURITY OPERATIONS CENTER

Centrum Operacyjne **SOC**

Usługa bieżącego monitorowania i analizy stanu bezpieczeństwa organizacji, zapewniająca szybkie wykrywanie cyberzagrożeń oraz natychmiastową reakcję na incydenty cyber

w trybie 24/7/365

- Monitorowanie sieci, systemów, aplikacji i urządzeń końcowych z wykorzystaniem narzędzi klasy SIEM i SOAR
- Analizowanie zdarzeń
- Eliminowanie zdarzeń false positive
- Wykrywanie incydentów
- Reagowanie na incydenty
- Zarządzanie podatnościami

WYKRYJEMY ZAGROŻENIA ZANIM ZADZIAŁAJĄ NA SZKODĘ TWOJEJ FIRMY

SKONTAKTUJ SIĘ Z NAMI

+48 22 243 39 37 kontakt@resilia.pl www.resilia.pl

O autorze

WOJCIECH CIEMSKI

Konsultant i trener cyberbezpieczeństwa, pasjonat bezpieczeństwa systemów i sieci oraz wszystkiego, co moglibyśmy zaliczyć do tak zwanego Blue Teamu. Autor bloga SecurityBezTabu.pl.

Nazywam się Wojciech Ciemski i jestem pasjonatem bezpieczeństwa systemów, sieci oraz wszystkiego, co moglibyśmy zaliczyć do tak zwanego Blue Teamu.
W branży IT zawodowo jestem od 2013 roku, gdzie zaczynałem jako pracownik pierwszej linii wsparcia. W swojej dotychczasowej karierze zawodowej byłem także specjalistą ds. IT, liderem zespołu ds. wsparcia, administratorem ds. utrzymania systemów, pełniłem rolę audytora wewnętrznego oraz byłem trenerem cyberbezpieczeństwa. Obecnie natomiast pracuje jako konsultant IT. Jestem również członkiem ISSA Polska.

Poza projektami, którymi zajmuje się w czasie mojej pracy zawodowej jestem prelegentem na imprezach zrzeszających specjalistów IT gdzie staram się promować wiedze dotyczącą bezpieczeństwa. Lubię się dzielić swoją wiedzą. Mam nadzieję, że mój blog i ta publikacja będzie najlepszym miejscem by mnie poznać, a dla Ciebie dobrym miejscem, żeby nauczyć się czegoś nowego.

Jeśli miałbyś do mnie jakiekolwiek pytanie to zapraszam do kontaktu przez formularz lub przez profil na LinkedIn. A może chcesz abym wystąpił na konferencji, w którą jesteś zaangażowany?

Rozdział 1

Wstęp

"Jeżeli jedyne narzędzie jakie znasz to młotek to każdy problem wygląda jak gwóźdź."

autor nieznany

Swoją przygodę z cyberbezpieczeństwem zacząłem w 2018, kiedy brałem aktywny udział w przygotowaniach do audytu certyfikującego ISO27001. Wtedy największym wyzwaniem przed jakim stanąłem, był właśnie wybór odpowiednich rozwiązań.

Spędziłem mnóstwo czasu nad testowaniem i wyborem odpowiednich narzędzi. Realizacja podnoszenia poziomu zabezpieczeń w systemach i sieciach nie zawsze wymaga istotnych nakładów finansowych. W tej publikacji przedstawię Ci narzędzia, które wspomagają mnie w mojej codziennej pracy oraz te warte uwagi.

Mam nadzieję, że dla Ciebie również okażą się pomocne.

Nie sposób niestety w publikacji tego typu pokazać Ci nawet niektóre z wariantów użycia wymienionych narzędzi. Potraktuj to jako dobry wstęp do dalszych poszukiwań.

Rozdział 2

Wybrane narzędzia

Sooty

[HTTPS://GITHUB.COM/THERESAFEWCONORS/SOOTY](https://github.com/theresafewconors/sooty)

Narzędzie wspomagające analityków SOC pozwalające na automatyzacje procesów - np. dokonywania rutynowych kontroli.

Peepdf

https://eternal-todo.com/tools/peepdf-pdf-analysis-tool

Narzędzie oparte o Pythona skanujące pliki PDF. Określa czy dany plik może być szkodliwy.

PyREBox

HTTPS://TALOSINTELLIGENCE.COM/PYREBOX

Sandbox (piaskownica) służący do inżynierii odwrotnej (reverse engeneering). Oparty jest na Pythonie. Pozwala na automatyzację.

Fail2Ban

https://www.fail2ban.org/wiki/index.php/Main_Page

Fail2ban skanuje logi serwera (np. ./var/log/apache/error_log) i banuje podejrzane adresy IP na podstawie zbyt wielu prób logowania, wyszukiwania podatności itd.

OSSEC

HTTPS://WWW.OSSEC.NET/

Otwartoźródłowa wielofunkcyjna platforma do nadzorowania pracy systemów. Zbiera logi i pomaga w tworzeniu SIEM, jak i wykrywa włamania.

RKHunter

HTTP://RKHUNTER.SOURCEFORGE.NET/

Linuksowe oprogramowanie ukierunkowane na wykrywanie rootkitów. Usuwa również niepotrzebne pliki i bada dostęp do konta roota. Obecnie przestarzały - ostatnia aktualizacja była w 2018 roku.

CHRookit

HTTP://CHKROOTKIT.ORG/

Narzędzie wykorzystujące proste linuksowe polecenia do wyszukiwania rootkitów. Może również być używany przy odzyskiwaniu danych z dysku.

Process Hacker

HTTPS://PROCESSHACKER.SOURCEFORGE.IO/DOWNLOADS.PHP

Pozwala na zarządzanie usługami i procesami w Windowsie. Służy również do wykrywania złośliwego oprogramowania. Jest napisany w C i posiada czytelne GUI.

Splunk

HTTPS://WWW.SPLUNK.COM/

Bardzo rozbudowane narzędzie, niezwykle ważne dla bezpieczników. Zbiera dane w czasie rzeczywistym i pozwala na przedstawianie ich w formie graficznej. Jest swego rodzaju dziennikiem danych.

Wazuh

HTTPS://WAZUH.COM/

Narzędzie wykrywające zagrożenia i pomagajace reagować na nie. Analizuje logi, ukryte pliki, nietypowe procesy i nie tylko.

TheHive

HTTPS://THEHIVE-PROJECT.ORG/

Platforma pozwalająca na zespołową pracę nad danym incydentem. Jest kompatybilne z MISP (Malware Information Sharing Platform).

Security Onion

HTTPS://SECURITYONIONSOLUTIONS.COM/

Dystrybucja Linuksa (oparta na Ubuntu) służąca do monitorowania ruchu w sieci. Opisuje poszczególne zdarzenia w sieci. W przypadku bardziej rozbudowanych sieci może wymagać dodatkowego fizycznego urządzenia.

CAINE

HTTPS://WWW.CAINE-LIVE.NET/

Dystrybucja Linuksa (oparta na Ubuntu) dostarczająca narzędzia do sprawnego i graficznego zbierania dowodów (forensics).

OSSIM

HTTPS://CYBERSECURITY.ATT.COM/PRODUCTS/OSSIM

Narzędzie działające jako SIEM, zajmujące się wykrywaniem i zapobieganiem atakom. Jest stworzone dla Linuksa, oparte na Debianie.

Prelude

HTTPS://WWW.PRELUDE-SIEM.ORG/

Służy jako SIEM. Zbiera dane i wiąże je ze sobą. Wspiera w działaniu wiele innych, pokrewnych programów.

Nagios

HTTPS://WWW.NAGIOS.ORG/

Służy do monitorowania stanu sieci - aktywnych hostów, systemów i aplikacji. Posiada czytelne GUI. Można go używać w przeglądarce. Nie wymaga wielu zasobów do działania.

Zabbix

HTTPS://WWW.ZABBIX.COM/NETWORK_MONITORING

Zabbix zbiera wiele rozmaitych danych, wykrywa nietypowy ruch w sieci, prezentuje graficznie dane w czasie rzeczywistym i nie tylko. Jest to aplikacja klasy enterprise, czyli wielozadaniowe dla rozwiązań biznesowych.

Icinga

HTTPS://ICINGA.COM/

Oprogramowanie oparte na Nagiosie, służące do monitorowania ruchu w sieci. Pozwala na współpracę z bazami danych.

Helk

https://github.com/Cyb3rWardog/Helk

Narzędzie służące do threat huntingu (tropienia zagrożeń), analizujące dane z wielu miejsc. Obecnie w fazie alpha.

CimSweep

HTTPS://GITHUB.COM/POWERSHELLMAFIA/CIMSWEEP

Zestaw narzędzi do PowerShella, dzięki któremu można lepiej reagować na zagrożenia. Obecnie przestarzały - ostatnia aktualizacja była w 2017 roku.

RedLine

https://www.fireeye.com/services/freeware/redline.html

Narzędzie od FireEye pozwalające na określanie zasięgu udanych ataków m.in. poprzez analizę procesów w systemie. Może służyć do zbierania IOC.

Yara

https://github.com/VirusTotal/yara

Yara pozwala na identyfikowanie i klasyfikowanie złośliwego oprogramowania różnego rodzaju. Działa na wielu systemach operacyjnych. Dzięki tworzeniu reguł można odizolowywać malware w czasie rzeczywistym.

Threat Ingestor

https://github.com/inquest/threatingestor

Zbiera IOC z ogólnodostępnych miejsc w internecie i wysyła je do odpowiednich systemów, np. SIEM.

Harden Tools

https://github.com/securitywithoutborders/hardentools

Hardening związany z funkcjami systemu Windows i aplikacjami Microsoft. Ogranicza pewne funkcjonalności na rzecz bezpieczeństwa.

Any Run

HTTPS://APP.ANY.RUN/

Pozwala na analizowanie podejrzanych plików bez konieczności tworzenia maszyny wirtualnej lub sandboxa. Można tam analizować w czasie rzeczywistym zagrożenia z wielu miejsc na świecie.

Hybrid Analysis

HTTPS://WWW.HYBRID-ANALYSIS.COM/

Narzędzie online analizujące pliki pod kątem zawartości złośliwego oprogramowania.

GoPhish

HTTPS://GETGOPHISH.COM/

Pozwala sprawdzić podatność danej organizacji na phishing.

SolarWinds

HTTPS://WWW.SOLARWINDS.COM/SECURITY-EVENT-MANAGER

SIEM z dodatkiem doświadczeń klientów SolarWinds, nastawiony na IOA.

Qualys VMDR 2.0

https://www.qualys.com/apps/vulnerability-management-detection-response/

Oprogramowanie nakierowane do ochrony infrastruktury krytycznej organizacji. Opisuje siebie samo jako zarządzanie podatnościami all-inclusive.

Network Reporting

https://www.shadowserver.org/what-we-do/network-reporting/

Raporty odnośnie aktualnych zagrożeń w cyberprzestrzeni.

Vulcan Cyber

HTTPS://VULCAN.IO/REMEDY-CLOUD

Baza danych zawierająca rozwiązania pozwalające na załatanie najpopularniejszych podatności i luk bezpieczeństwa.

Ransomware Risk Assessment

HTTPS://TESTMYDEFENSES.COM

Przeprowadza testy zabezpieczeń, pokazując przy tym zagrożenia i podatności.

CISA Cybersecurity Publications

https://www.cisa.gov/subscribe-updates-cisa

Newsletter CISA.

Immunet Antivirus

HTTPS://WWW.IMMUNET.COM/

Oprogramowanie działające jako antywirus, gdzie zagrożenia są zgłaszane przez społeczność.

Cloudflare Unmetered Distributed Denial of Service Protection

HTTPS://WWW.CLOUDFLARE.COM/PLANS/FREE/

Oprogramowanie chroniące przed atakami DDOS od Cloudflare.

Microsoft Defender Application Guard

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview

Pozwala na otworzenie przeglądarki Microsoft Edge w odizolowanym środowisku.

Controlled folder access

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders

Chroni foldery i pliki przed niautoryzowanymi zmianami przez aplikacje.

Microsoft Defender Antivirus

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows

Wbudowane narzędzie w najnowsze systemy Windows, które jest można traktować jako domyślnego antywirusa. Wykrywa różne rodzaje złośliwego oprogramowania.

PGP

https://www.openpgp.org/

Szyfruje maile z wykorzystaniem architektury klucza publicznego.

BitLocker for Microsoft Windows

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

Używa się go do szyfrowania w systemach Windows.

Quad9

HTTPS://QUAD9.NET/

Blokuje dostęp do stron, które mogą zawierać złośliwe oprogramowanie lub służyć jako phishing.

AllStar

https://github.com/ossf/allstar

Wymusza na urządzeniach działanie zgodnie z określoną polityką bezpieczeństwa organizacji.

Open Source Insights

HTTPS://DEPS.DEV/

Pokazuje zależności pakietów od innego oprogramowania.

Tink

https://github.com/google/tink

Biblioteka zajmująca się bezpieczeństwem API.

Tsunami Security Scanner

https://github.com/google/tsunami-security-scanner

Jest to skaner wykrywający podatności. Obecnie w fazie "pre-alpha".

OpenDNS Home

HTTPS://SIGNUP.OPENDNS.COM/HOMEFREE/

DNS, który domyślnie blokuje strony mające na celu phishing.

Cyber Security Ratings

https://securityscorecard.com/instant-security-scorecard

Określa stopień bezpieczeństwa danej organizacji w skali 0-100.

Atomic Red Team

HTTPS://ATOMICREDTEAM.IO/

Przeprowadza testy oparte na macierzy MITRE ATT&CK.

CrowdStrike CRT

https://www.crowdstrike.com/resources/community-tools/crt-crowdstrike-reporting-tool-for-azure/

Pozwala na zobaczenie stopnia dostępu do określonych zasobów w Azure AD.

Tenable Nessus Essentials

https://www.tenable.com/products/nessus/nessus-essentials

Sprawdza podatności np. w architekturze klient-serwer.

Alien Labs Open Threat Exchange (OTX) Endpoint Security

HTTPS://CYBERSECURITY.ATT.COM/OPEN-THREAT-EXCHANGE

Sprawdza endpointy pod względem IOC.

Kali Linux

HTTPS://WWW.KALI.ORG/

Dystrybucja Linuksa przeznaczona do testów penetracyjnych i innych red teamowych działań.

RiskIQ Community

HTTPS://COMMUNITY.RISKIQ.COM/HOME

Zbiór bieżących informacji dotyczących złośliwego oprogramowania.

Splunk Synthetic Adversarial Log Objects (SALO)

https://github.com/splunk/salo

Oprogramowanie służące do generowania logów.

Carbon Black TAU Excel 4 Macro Analysis

HTTPS://COMMUNITY.CARBONBLACK.COM/

Platforma pozwalająca na wymianę doświadczeń odnośnie obecnie trwających ataków.

Paros Proxy

HTTPS://WWW.PAROSPROXY.ORG/

Oprogramowanie oparte na Javie służące do znajdowania podatności.

Let's Encrypt

https://letsencrypt.org/getting-started/

Pozwala tworzyć darmowe certyfikaty SSL.

Hping

HTTP://WWW.HPING.ORG/

Oprogramowanie wysyłające sprecyzowane pakiety TCP, UDP lub ICMP pozwalające na sprawdzenie poziomu bezpieczeństwa.

Aircrack

https://www.aircrack-ng.org/

Oprogramowanie pozwalające na testowanie haseł w sieciach Wi-Fi.

w3af

HTTP://W3AF.ORG/

Oprogramowanie służące do znajdowania podatności w aplikacjach webowych.

Vane2

https://github.com/delvelabs/vane2

Skaner podatności dla WordPressa.

Checkov

https://www.checkov.io/

Skaner podatności dla rozwiązań chmurowych.

Zed Attack Proxy (ZAP)

HTTPS://WWW.ZAPROXY.ORG/

Oprogramowanie służące do znajdowania podatności w aplikacjach webowych.

nmap

HTTPS://NMAP.ORG

Oprogramowanie służące do skanowania portów.

Perception Point

HTTPS://PERCEPTION-POINT.IO/EMAIL-SECURITY-FREE-PLAN/

Chroni organizacje przed atakami za pomocą poczty elektronicznej.

Semperis Purple Knight

HTTPS://WWW.PURPLE-KNIGHT.COM/

Oprogramowanie wykrywające podatności w konfiguracji Active Directory.

Microsoft Safety Scanner

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide

Wykrywa złośliwe oprogramowanie w Windowsach.

Google Safe Browsing

HTTPS://SAFEBROWSING.GOOGLE.COM/

Ostrzega o potencjalnym zagrożeniu podczas przeglądania Internetu. Wbudowane w Androida i Google Chrome.

Malcolm

https://github.com/idaholab/Malcolm

Pozwala na analizowanie ruchu sieciowego z plików .pcap i nie tylko.

Madiant

https://github.com/mandiant

Zbiór narzędzi pozwalających na znalezienie IOC.

VirusTotal

HTTPS://WWW.VIRUSTOTAL.COM/GUI/HOME/UPLOAD

Pozwala na analizę pod kątem złośliwego oprogramowania zarówno plików, jak i URL.

Netfilter

HTTPS://WWW.NETFILTER.ORG/

Analizuje pakiety i pozwala na konfigurację firewalla. Przeznaczony dla dystrybucji Linuksa.

Wireshark

HTTPS://WWW.WIRESHARK.ORG/

Najpopularniejszy sniffer dostępny na wielu systemach. Pozwala również na analizę pakietów z wykorzystaniem różnych filtrów.

Ettercap

HTTP://ETTERCAP.SOURCEFORGE.NET/

Pozwala na analizę ruchu sieciowego, jak i podszywanie się pod adresy MAC/IP, dzięki czemu można przeprowadzić atak MITM.

Kismet

https://www.kismetwireless.net/

Kismet pozwala na pasywne skanowanie sieci, jak i wykrywanie incydentów bezpieczeństwa. Przeznaczony do sieci WiFi.

Snort

HTTPS://WWW.SNORT.ORG/

Rozbudowana aplikacja pozwalająca np. na wykrywanie intruzów w sieci. Dostępna na wielu dystrybucjach Linuksa.

sqlmap

HTTP://SQLMAP.ORG/

Przeprowadza ataki typu SQL Injection, dzięki czemu można wykryć podatności.

RITA

https://www.activecountermeasures.com/free-tools/rita/

Narzędzie typowo defensywne, pozwalające na wykrycie prób ataków poprzez analizę ruchu sieciowego.

Dalton

https://github.com/secureworks/dalton

Pozwala na odtworzenie ruchu z plików .pcap trzymając się zdefiniowanych wcześniej zasad.

Elastic SIEM

https://www.elastic.co/blog/elastic-siem-free-open

Darmowy, rozbudowany SIEM.

OpenSSH

https://www.openssh.com/

Pozwala na łączenie się za pomocą SSH.

VMware Workstation Player

HTTPS://WWW.VMWARE.COM/CONTENT/VMWARE/VMWARE-PUBLISHED-SITES/US/PRODUCTS/WORKSTATION-PLAYER/WORKSTATION-PLAYER-EVALUATION.HTML.HTML

Tworzy pojedynczą wirtualną maszynę na Windowsie lub dystrybucji Linuksa.

John the Ripper Password Cracker

https://www.openwall.com/john/

Oprogramowanie łamiące hasła. Może posłużyć jako tester zabezpieczeń w organizacji.

Trusona

https://docs.trusona.com/totp/overview/

Pozwala na dwuetapową weryfikację. Aplikacja jest dostępna zarówno w Google Play Store i Apple App Store.

Windows Auto-Backup

https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-352091d2-bb9d-3ea3-ed18-52ef2b88cbef

Odnośnik do konfiguracji automatycznych kopii bezpieczeństwa dla systemów Windows 10 i 11.

Microsoft Threat Modeling Tool

https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Narzędzie pozwalające na threat modeling (modelowanie zagrożeń).

Jeśli uważasz tę pozycję za wartościową to podziel się nią dalej!

:)